Polarization Entanglement Quantum Key Distribution with Covert Classical Communications

John Gariano and Ivan Djordjevic
Department of Electrical and Computer Engineering
The University of Arizona
Tucson, Arizona, 85721, USA
Email: Jagariano@email.arizona.edu

***Abstract*—By using a covert classical communication channel for error reconciliation in QKD systems, higher SKRs are capable of being achieved. Assuming transmission over a 30km maritime channel, our previous results for the selection of optimum wavelength for use are re-examined.**

I. Introduction and QKD System

In our previous work, a polarization entangled quantum key distribution (QKD) system using the standard BB84 protocol was presented considering the optimum wavelength selection for a 30 km Maritime channel where the transmit/receive apparatus is located on a mast 50m above the water [1]. The 10%, 50% and 90% occurrence of the channel are considered. Entangled photons are assumed to be generated using a Type II spontaneous parametric down conversion source (SPDC) at 780nm, 1550nm, and 4µm. Two periodically poled $LiNbO_3$ (PPLN) crystals located before Alice's and Bob's detection system are used to convert the 780nm and 4µm wavelengths to 1550nm with maximum conversion efficiency of 0.9, where they can be detected by the NuCrypt CPDS 1000 with detection efficiency of 0.2 [2]. The system being studied is depicted in Figure 1, where the source is located at Alice and the eavesdropper, Eve, is located in the channel between Alice and Bob.

A key performance metric of a QKD system is the secure key rate (SKR). To calculate the SKR, the security proof given by Koashi and Preskill is used, shown in Equation 1 [3]

$$R_{SKR} = P_{Key}\left[1 - f(\delta)H_2(\delta) - H_2(\delta)\right], \tag{1}$$

where P_{Key} is the probability of a time slot being included in the unsecured key, δ is the bit error rate (BER), $H_2(\delta)$ is he binary entropy function, and $f(\delta)$ is the error reconciliation efficiency, where $F(\delta) \geq 1$. During the error correction process, the parity bits are transmitted through a public channel with no error. This reveals additional information to Eve. If an error correction code that has ideal error reconciliation efficiency $(f(\delta) = 1)$ is used, the SKR scales as $R_{SKR} = P_{Key}\left[1 - 2H_2(\delta)\right]$.

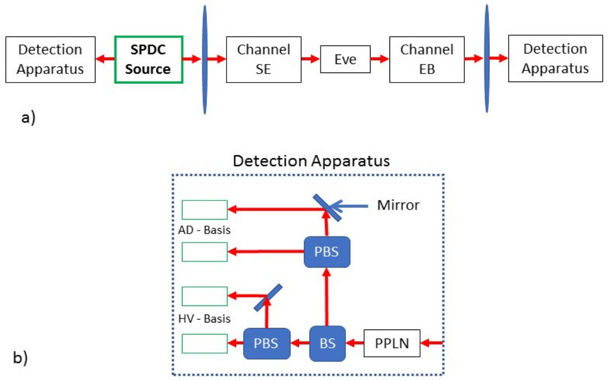

Fig. 1: a) System Diagram: The photon transmitted to Bob first passes through a channel between the Source and Eve (channel SE), where Eve is assumed to be able to correct all distortions. Then it passes through a channel between Eve and Bob (Channel EB). b) Detection apparatus: implementing the BB84 protocol using a beam splitter to randomly place photons in either the HV or AD basis

II. Covert Communication

One way to improve the secure key rate is to use a covert communication channel in place of the public channel. Covert communication is the process of transmitting a message between two authenticated users, Alice and Bob, without being detected by a third party, Eve. The concept of covert digital communication was present by Boulat Bash in 2013, where the message is transmitted below the noise floor [4], [5]. One method for transmitting below the noise floor is by using spread spectrum techniques such as direct sequence spread spectrum (DSSS) and frequency-hopping spread spectrum

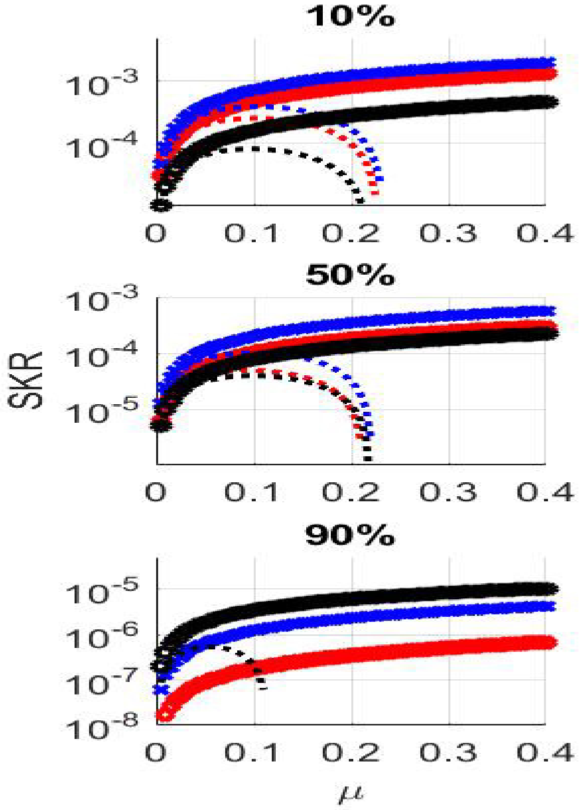

Fig. 2: SKR of full system using detector lengths of 20μm and assuming Eve does not perform the intercept resend attack against average number of photons sent μ for various wavelengths. The wavelengths are as follows: 780nm red, 1550nm blue, 4μm black, dashed lines represent the SKR calculation using a classical public channel

(FHSS). However for an additive white Gaussian noise channel (AWGN), only $\mathcal{O}(\sqrt{n})$ bits can be transmitted covertly in n channel uses, thus the rate goes to 0 as n tends to infinity. This is due to Alice having to decrease her transmit power, as the number of channel increases allowing Eve to gains more information on the channel. To allow for positive covert communication rates, a jammer can be used to introduce noise to both Bob and Eve, and allowing to Alice to transmit with a non-decreasing power [6]. By transmitting the message over a channel below the noise floor, errors will be introduced. To compensate for these errors an additional forward error correction code, with high error correction capabilities, is used to encode the parity bit before transmission. This results in no information leakage to Eve regarding the parity bits and the SKR now scales as $R_{SKR} = P_{Key}\left[1 - H_2(\delta)\right]$.

III. Results

Using the same data from our previous work, the new SKR is calculated assuming that a covert classical communication channel is used. In all cases the SKR has increased, and higher average number of photons sent can be used, as can be seen in Figure 2. The maximum BER to achieve a non-zero SKR was previously 0.11, while new maximum is 0.5. It should also be noted that channels with loss so high no SKR was achievable are now capable of generating non-zero SKR. As previously mentioned, due to higher channel loss and increased wavefront distortion the SKR decreases for the 50% and 90% occurrences. Additionally, as the effects of turbulence strength increases, less distortion is introduced for longer wavelengths, making them the optimal wavelength selection in strong turbulence.

IV. Conclusion

The use of a covert classical communication channel enables Alice and Bob to reconcile errors in their shared key without revealing information to Eve. With a classical public channel, the maximum BER was 0.11, while with a covert communication channel, the maximum BER is 0.5, and the practical limitation will be the error correction capability of the error correction codes. This increase in maximum BER allows for non-zeros SKR to be achieved when the channel has very high loss or noise. As in our previous work, the optimal wavelength selection has remained the same.

Funding Information

ONR MURI program (N00014-13-1-0627)

References

[1] J. Gariano, I. Djordjevic, and T. Liu, "Optimal wavelength selection for entangled quantum key distribution," pp. 721–722, IEEE, 2017.

[2] M. A. Albota and F. N. C. Wong, "Efficient single-photon counting at 1.55 μ m by means of frequency upconversion," *Opt. Lett.*, vol. 29, pp. 1449–1451, Jul 2004.

[3] M. Koashi and J. Preskill, "Secure quantum key distribution with an uncharacterized source," *Phys. Rev. Lett.*, vol. 90, p. 057902, Feb 2003.

[4] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on awgn channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1921–1930, September 2013.

[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, pp. 26–31, Dec 2015.

[6] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 6193–6206, Sept 2017.